

How to detect keyloggers on smartphones

If you rely on your phone to access your bank accounts, enter sensitive messages, pay bills, or even unlock your house, a smartphone keylogger can steal this information without you even knowing. .

Cybercriminals can use keyloggers to learn your passwords, credit card numbers, etc. - so you should know how to detect and prevent these threats to keep your phone activities private. your smartphone.

What is a keylogger?



Keylogger is software that tracks your keystrokes. Whenever you type something, it records the buttons you press and the order in which you press them. Some businesses use keyloggers to hold employees accountable during work hours, but malicious versions help hackers steal your information.

You may be familiar with PC versions like Snake Keylogger, which infects Microsoft Office or PDF readers, but keyloggers can also target your phone.

Smartphone keyloggers can be even more dangerous than their desktop counterparts because phone security is so easy to bypass. Most people are familiar with antivirus protection and similar protections on their computers, but phones are a different matter.

Many people miss the need for phone security because the iPhone doesn't necessarily need an antivirus app. That's because they have strong built-in protections, and the design of iOS makes many attacks unlikely unless the phone is jailbroken. In contrast, Android is more vulnerable to attacks.

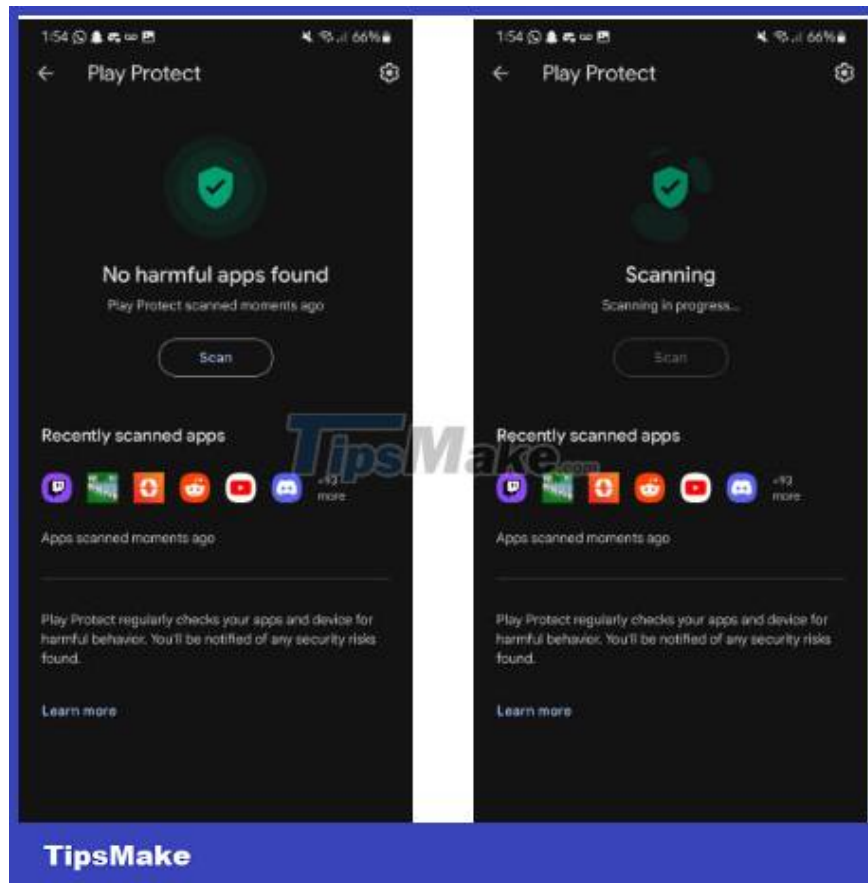
How to detect Keylogger on smartphone

Keyloggers can be more difficult to detect than other types of malware. That said, keyloggers have some telltale signs that need attention.

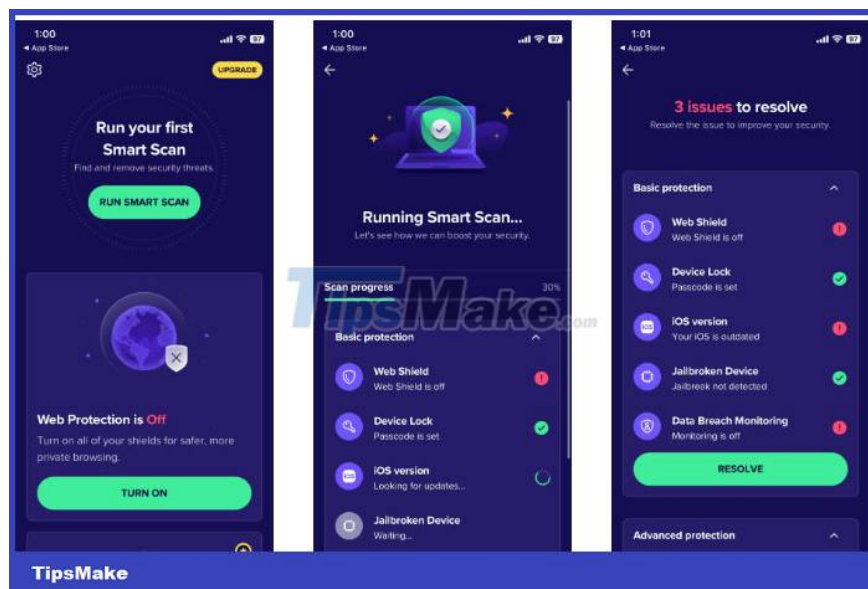
1. One of the biggest signs of a keylogger is lag when you type. It's a red flag if your input takes time to display after you tap something. This comes from malware recording keystrokes and taking up processing power.
2. Likewise, pay attention to whether performance is reduced. Slow response times, app crashes, and graphics not loading are all warning signs. They're a sign that your phone is doing more processing than usual, especially if it seems to be happening out of the blue.
3. Overheating is another sign of a smartphone keylogger, as it often occurs when everything is running in the background. It would be worrying if you don't have any apps open but your phone is heating up. The same thing happens when battery life drains unusually quickly or your smartphone uses more data than usual.

Restart your phone if you notice any of these signs. If that doesn't fix the problem, the cause may be a keylogger. Google Play Protect Scan can scan dangerous apps on Android to identify malware.

To run Google Play Protect Scan, open the Google Play Store, tap your profile icon, select 'Play Protect', then tap the gear icon to open its settings. Enable 'Scan apps with Play Protect' if you haven't done so already, then return to the main Play Protect page and tap Scan. Your phone will then scan for malware and unknown apps, suggesting next steps if anything is found.



Apple devices don't have such a built-in feature (mainly because iOS doesn't suffer from the same malware as Android), but you can download a trusted third-party security app like Avast or Norton 360 to scan your iPhone. Both apps are free to download, although Avast offers free scanning without needing to set up a subscription or free trial:



Note that iOS devices are not impervious to malware, ransomware, and keyloggers; it's just much rarer and usually involves a jailbroken device or being highly targeted (using something like Pegasus spyware).

How to remove keylogger from smartphone



Once you have identified the keylogger on your smartphone, you have several options for removing it. The easiest way is to use whatever security app you use to scan for malware. Once the scan detects the keylogger, it will give you the option to remove the software. Do that and reboot your phone afterwards.

You can also search for and remove suspicious apps manually. Anything you don't download from the official app store falls within that range. The same goes for any app where you notice a significant drop in performance after downloading. If the problem arises after installing a certain app, remove it. If not, go into the app list in your phone's settings and delete anything you don't remember downloading.

You can try factory reset if neither of the above steps work. There are several ways to factory reset Android and iPhone, but no matter how you do it, remember to back up your important files first. Resetting will delete all unimportant data, including keyloggers.

You finished reading the article "**How to detect keyloggers on smartphones**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.